

CONSENT AND CONFIDENTIALITY — LEGAL IMPLICATIONS OF ELECTRONIC TRANSMISSION OF PRESCRIPTIONS

By *Joy Wingfield, LL.M., FRPharmS, and Charles Foster, Barrister*

In this article the authors discuss, from pharmaceutical and legal viewpoints, issues surrounding the replacement of traditional paper prescriptions by electronic transmission of prescriptions in community pharmacies

The courts and the textbook writers have spent much time and energy on medical confidentiality, but there is not much material which deals specifically with pharmacists. One notable exception is the cornerstone case in the Court of Appeal about the use of anonymised data from patient medication records (the "Source Informatics" case¹⁻³). Consent-to-treatment issues have until recently hardly affected pharmacists for the simple reason that pharmacists have traditionally not been much involved in initiating treatment where consent might be an issue. But pharmacists can no longer avoid grappling with issues of consent in another context: consent to the use of personal data.

Some work has been undertaken⁴⁻⁶ researching the views of patients and health care professionals about the sharing of patients' clinical information, but the perspectives have been mostly those of social scientists and ethicists rather than lawyers. Several new statutes — the Data Protection Act 1998, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Health and Social Care Act 2001 — have significant implications for the use of clinical data. Consent issues in medicine have been under intense media scrutiny.⁷⁻⁹ People increasingly want to know what information is held about them, why it is held, and what it is used for. Extensive consultation and deliberation has resulted in an avalanche of guidance from civil service desks and professional bodies,^{10,11} but little makes any direct reference to community pharmacy. As community pharmacists become increasingly integrated into the patient care team and gain access to an ever greater quantity and range of sensitive clinical data (needed for medicines management or supplementary prescribing, for example), they are increasingly likely to run into the principles of data protection and the law on confidentiality and consent. This article

looks through legal* and pharmaceutical eyes at one area of increasing importance: the replacement of traditional paper prescriptions in community pharmacies by electronic transmission of prescriptions (ETP).^{12,13}

HEALTH CARE LAW AND CONFIDENTIALITY

It has long been recognised that it is important to maintain confidentiality between patient and health care professional. Patients often do not want their names, addresses and ages, let alone their intimate secrets, to be broadcast. If patients think that their secrets will not be respected by the doctor they will be reluctant to be as candid with the doctor as is clinically necessary. The English common law has long acknowledged an "obligation of confidence", owed by doctors and many other professionals, and statutes such as the Data Protection Acts have deployed the criminal law to regulate some uses of sensitive personal data. If a health care professional breaches a patient's confidence he or she might be sued for damages for breach of confidence, disciplined by his or her professional regulatory body and, in some circumstances, be liable to a criminal penalty.

The duty of confidence is not absolute. There is a public interest in maintaining confidence: there may sometimes be a public interest in breaching it. Often actions for breach of clinical confidence are determined by the judge deciding whether the public interest in non-disclosure is outweighed by the public interest in disclosure.

Where a professional is sued for breach of confidence, the court will always look carefully at what the relevant professional disciplinary body says about disclosure in the relevant circumstances. If the disciplinary body would excuse disclosure, the court is likely to do so also. If the disciplinary body would condemn disclosure, the court is likely to do so, too. The converse does not follow: the English disciplinary bodies are generally harder on their members than the courts are.

The Human Rights Act 1998 has the effect of grafting into the English law the

European Convention on Human Rights. Article 8 of the Convention provides, insofar as relevant: "1. Everyone has the right to respect for his private and family life. . . 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Article 8(1) includes a right not to have one's private information disseminated. But this is not an absolute right. It is qualified by article 8(2). Whether one expresses the law of confidentiality in the old way (duties not to disclose, qualified by excuses for disclosing in the public interest) or the new European way (a right not to have secrets disclosed, but a right qualified by the wider demands of society) it comes to much the same thing. The Human Rights Act might well help to carve out a new law of privacy, but in the realm of clinical confidences it is unlikely to change much more than the language used by lawyers to describe the old problems. It has, however, made patients more aware of the rights which they have always had.

The recent case of Source Informatics (see above), in which both traditional and European rights' analyses were considered, concluded that a breach of confidence would be actionable if the disclosure would be regarded as "unconscionable". Since any person of conscience, in deciding whether or not disclosure of clinical information was justified, would weigh the patients' concerns against the wider interest in disclosure, the net result is the same as it would have been under the old established law.

Professor Wingfield is Boots Special Professor of Pharmacy Law and Ethics at the Pharmacy School, University of Nottingham, Nottingham NG7 2RD. Mr Foster is a barrister at 6 Pump Court, Temple, London EC4Y 7AR. Correspondence to Professor Wingfield (e-mail joy.wingfield@nottingham.ac.uk)

*All legislation referred to applies to England and Wales. The Data Protection and Human Rights Acts apply to Scotland and Northern Ireland, as does most of the Freedom of Information Act. The Health and Social Care Act, including section 60, only applies to England and Wales.

HEALTH CARE LAW AND CONSENT TO THE COLLECTION, PROCESSING AND RETENTION OF PERSONAL DATA

Medical law has traditionally thought about consent in the context of consent to treatment. Treating a patient without the necessary consent might lead to an action for damages, to criminal prosecution for trespass to the person, or to censure by the professional regulatory organisation. But that is not the only health care context in which consent is relevant. It is obvious that patients need to give their consent to some uses of their personal data. Of course that was always true. In the law of confidentiality a patient could not sue a clinician for breach of confidence if the patient had consented to the disclosure that had occurred. The patient would generally be assumed to have consented to the disclosure to the necessary clinicians of those elements of the collected data necessary for diagnosis and treatment. But the issues of confidentiality and consent were not often mentioned in the same mental sentence until the first Data Protection Act in 1984.

This Act was prompted by concerns about personal data held on computers. It defined the principles of fair data collection and the circumstances in which collection and retention would be unlawful. The Data Protection Act 1998 (a consolidating Act in which the 1984 Act is subsumed) makes it unlawful to "process" personal data at all, whether on paper or electronically, unless certain prerequisites are met. These conditions are set out in Schedules 1, 2 and 3 of the Data Protection Act 1998.¹⁴

Schedule 1 The first of the "data protection principles", set out in Schedule 1, is that "personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: (a) at least one of the conditions in Schedule 2 is met; and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met." "Sensitive personal data" includes "personal data consisting of information as to [the data subject's] physical or mental health or condition".¹⁵ Information supplied to pharmacists is therefore "sensitive personal data".

Schedule 2 What Schedule 2 conditions might apply in a dispensing situation? Condition 1 requires that the data subject has given his consent to the processing. By handing over a prescription, implied consent might well be deemed to have been given. If consent were not deemed to have been given there are several other conditions which make lawful the processing of personal data during the dispensing process. Condition 2(a) is: "the processing is necessary for the performance of a contract to which the data subject is a party". Dispensing is carried out under an NHS contract for which personal data are needed. Similarly, during dispensing, pharmacists are legally obliged to take and hold some information about patients for whom they dispense and could claim exemption from the need for consent under condition 3, "the processing

is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract". Condition 5(b) is "the processing is necessary for the exercise of any functions conferred on any person by or under an enactment" and 5(d) is "... for the exercise of any other functions of a public nature exercised in the public interest by any person". Again dispensing is carried out under an NHS contract laid down in statute and pharmacists dispense under powers given to them by statute. This does not mean, though, that they can validly process any patient information. They can only process insofar as it is necessary for the exercise of their statutory function. Condition 6 is a catch-all: "The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject." Lawful dispensing is obviously a "legitimate interest".

What this comes to is that most processing by pharmacists of sensitive personal data will easily satisfy one or more of the Schedule 2 conditions. But some of it may not: the key word is "necessary". This issue is returned to below.

Schedule 3 Having satisfied the Schedule 2 filter, one of the Schedule 3 conditions must also be satisfied in order to make the pharmacist's processing of sensitive personal data lawful.

The first Condition in Schedule 3 is that "the data subject has given his *explicit consent* to the processing of the personal data" (our italics). This is unlikely to be the case in current dispensing practice. Although there are several conditions which could be considered applicable as in Schedule 2, the most pertinent is to be found in Condition 8. This says: "(1) The processing is necessary for medical purposes and is undertaken by (a) a health professional; or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional. (2) In this paragraph 'medical purposes' includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services."

In summary, therefore, to be fair and lawful, personal data may only be processed with the consent of the "data subject" or within the terms of exemptions set out in the Schedules. Moreover the processing of personal data, even in health care, must be fair and transparent and, wherever possible, patients must be given the option of limiting the spread and use of their personal health care details.

There are three points to note from the above analysis. First, the Data Protection Act 1998 specifically includes pharmacists in the definitions of "health professional".¹⁶ Second, the use of the word "necessary" in both schedules implies that anonymised or pseu-

donymised data for processing should be preferred wherever possible. Third, despite point 2, the exemptions generally embody common sense and ancient presumption by assuming that by presenting for consultation, a patient implies consent to subsequent necessary exchange of information — necessity being determined by the health care provider who in turn is subject to the common law duty to keep confidences and his own professional disciplinary jurisdiction.

A lot of media attention has been focused on the sinister potential of section 60 of the Health and Social Care Act 2001, which provides that "the Secretary of State [for Health] may by Regulations make such provision for and in connection with requiring or regulating the processing of prescribed patient information for medical purposes as he considers necessary or expedient (a) in the interests of improving patient care or (b) in the public interest". The Government has said that this Section is intended to make data available for legitimate research and has tried to reassure worried commentators that patient confidentiality will not be a casualty of the section. Many are unconvinced.^{7,17-19} The first Order under this section has now been made²⁰ and future regulation may be forthcoming to address the reservations expressed by the Department of Health during the Source Informatics case concerning the sale of data from patient medication records (PMRs). It remains to be seen how Section 60 will affect the law of clinical confidentiality.

HEALTH CARE LAW AND TRADITIONAL DISPENSING

Consent issues can arise at all stages of the prescribing and dispensing process. It is reasonable to assume that, by presenting for a consultation, a patient implicitly consents to his personal data being entered on the surgery computer and subsequently transferred, along with details of the prescribed medication, to a prescription form. By presenting that prescription to an NHS contracted pharmacy, the patient also implicitly consents to those data being used to enable the prescription to be dispensed. But does the patient have to consent explicitly to his data being stored in the PMRs? The answer from the (then) Data Protection Registrar has been "no", even for PMRs pooled by national networks of pharmacies with access by individual pharmacies within that network, provided that the use of the data was consistent with the registered purpose of health care provision (personal communication). This position is now confirmed in statute at least in relation to most of the data routinely supplied and recorded during traditional dispensing.

Consent to two further processes should be considered. The first we will call fulfilment. Fulfilment is an American term now being adopted in the United Kingdom to mean confirmation of the dispensing of a prescription at a specific pharmacy. Such information is already transmitted informally on an individual basis when a pharmacy contacts a surgery and gives this

confirmation. Disclosure of such information is rarely contentious and explicit consent is not routinely sought. Almost certainly, transmission of most such information falls squarely within the exemption in Schedule 3 paragraph 8 of the Data Protection Act 1998. Remember, though, that it is only transmission of necessary information which is lawful.

The second possible process is access to diagnosis. At the time of presentation of the prescription, the diagnosis is frequently apparent to the pharmacist (and sometimes to others) from the medication prescribed. But inference from the medication is not the only way in which pharmacists might get information about diagnosis. All community pharmacies now keep PMRs. As well as recording medication data obtained directly from the prescription, PMRs often include information provided by the patient or a proxy, such as details of allergies, special requirements, clarification of ambiguities and explicit confirmation of the diagnosis.

Information about diagnosis is often conveyed when pharmacists query prescriptions. When queries arise on prescriptions, most pharmacists attempt to clarify them first with the patient or proxy. Diagnosis might be mentioned or necessarily implied in the response. If the patient or proxy does not make things clear, the pharmacist will often telephone the surgery and speak to the prescriber or a member of staff. It is often presumed (generally correctly) that the patient would wish, or even expect, this exchange to take place although confirmation is often sought informally: "I'll just need to speak to the surgery, is that OK?" Thus most patients expect consultation between pharmacist and prescriber (and vice versa) in which the diagnosis is likely to become apparent. No empirical data exist as to whether or to what extent patients, or the wider public, are aware of the access pharmacists may have to diagnosis. Certainly, such access does not require explicit consent if the prerequisites of Schedule 3 paragraph 8 of the Data Protection Act 1998 are met. Pharmacists argue that they require access to diagnostic and biochemical results such as international normalised ratios, forced expiratory volume readings, blood glucose levels, etc, in order to interpret prescriptions intelligently and to make or recommend any appropriate adjustments to prescribed medication. However, to be lawful, pharmacists (and indeed nurses or any others who may run clinics) must be prepared to defend such access as necessary in each case to claim exemption under paragraph 8 of Schedule 3. If such processing is not necessary, then it will not be lawful without explicit consent from the data subject.

WHAT DOES AND DOES NOT CHANGE WITH ETP?

ETP allows the creation of a prescription in an electronic form and transmission of prescription data electronically to the chosen dispensing pharmacy. These data are used to create a label and a PMR. No new issues of consent or confidentiality arise from ETP. It is hoped that the electronic records created

will ultimately be in a standard format and therefore uniformly accessible by all ETP users. They should facilitate tedious processes such as pharmaceutical audit and the mechanics of repeat dispensing. The advent of ETP creates the prospect of increased ease of access by community pharmacists to much more medical data (such as diagnostic information and biochemical test results). Such access is commonplace for hospital pharmacists and increasingly for pharmacists working in general practitioners' surgeries. Whether this access is necessary or not (and therefore legal or not) has been discussed above.

In 1997, the professional bodies for medicine and pharmacy recognised that ETP might have adverse effects on patient confidentiality. A joint statement of key principles to be followed for ETP²¹ includes a requirement that "the system must not permit the direction by doctors, pharmacists or pharmacies of prescriptions to a specific pharmacy or group of pharmacies". The mechanisms for transfer of data in the two "push" models of ETP (see below) are therefore not consistent with this principle. The joint statement, and a later one approved at the International Pharmaceutical Federation Congress in Singapore in 2001,^{22,23} also stresses the need to raise awareness and ensure consent from patients to the transfer of, and access to, their data via ETP.

DATA MANAGEMENT IN THE VARIOUS ETP MODELS

Two of the three pilots, Pharmacy2u and Transcript, use what is called a "push" model of data transmission in which the prescription data, in an encrypted electronic form, is "pushed" from the GP surgery to the pharmacy chosen by the patient to dispense the prescription. In the third pilot, being run by Flexiscript, the data are encrypted and held on an interim basis in a "relay" — a kind of electronic holding bay — from which a pharmacy may "pull" the relevant prescription data when a patient chooses to call at the pharmacy for the dispensing of the prescription. In all cases, the data are encrypted when they leave the control of the GP and can only be decrypted by appropriate health professionals or their staff. These measures are consistent with the spirit and the letter of the Data Protection Act 1998 in stopping data going to anyone apart from people who need to see it. It would presumably be possible, by insisting on the use of structured electronic forms, to reduce the risk of unnecessary (and therefore unlawfully processed) data being transferred. If, for example, it were decided in principle that pharmacists should not be processing certain diagnostic information, or not in certain circumstances, it should be possible simply to exclude such information from the information available for decryption.

THE ROLE OF THE DATA CONTROLLER

The Data Protection Act 1998 defines the data controller as the person who determines the purposes for which and the man-

ner in which personal data are, or are to be, processed.²⁴ Where personal data are processed only for purposes for which they are required by or under an enactment (which might be the case for data processed for the purpose of dispensing) the data controller is the person on whom the enactment imposes the obligation to process the data.²⁵ In the ETP pilots, the data controllers are the GPs and pharmacists who are collaborating in the trial. In any ETP system, just as in a more conventional system, the controller must ensure that decryption and access are restricted to those who have a "health professional or equivalent" duty of confidentiality and care.

FAIR AND LAWFUL PROCESSING

The first principle of data protection (Schedule 1) states that data must be processed "fairly and lawfully". Part II (1) of this Schedule says that, in determining whether data are processed fairly, "regard is to be had as to the method by which [the data] are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed". ETP is not so revolutionary an idea: if and insofar as the data processed for the purposes of conventional dispensing are lawfully processed, data processed in the course of ETP will probably be lawfully processed, too.

But it is clearly desirable that the data-providing public should know more than they presently do about what is done with their personal details. In the opinion of the Office of the Data Protection (now Information) Commissioner,²⁶ the NHS should become far more transparent about its uses and disclosures of confidential patient information. In response to this opinion, a far-reaching report commissioned from Cambridge Health Informatics (now incorporated into an NHS Information Policy Unit Strategy document)²⁷ recommended a public communication campaign to increase transparency and build patient confidence in the NHS and its staff. This is even more important when the NHS services involve the private sector. Although some research on patient attitudes is referred to in the Cambridge report, there have been few large scale studies of the transmission or sharing of information between GPs and community pharmacies, and none as yet relating to the effect of electronic transmission (although it is understood that this will be part of the evaluation of the three pilots).

DATA TRANSMITTED SO THAT PHARMACISTS GET PAID

The current NHS prescription form also acts as an invoice for the remuneration of community pharmacy contractors. The prescriptions are currently sent by post to the prescription pricing bodies. Sometimes they go missing. Transmission of the same data by ETP should be more secure. Provided that adequate safeguards to protect confi-

deniality are built into the transmission system (which would not be technically difficult), electronic transmission of necessary data would fall into one of the Data Protection Act 1998 exempted categories and would not require explicit patient consent.

RETENTION OF DATA

The Data Protection Act 1998 (principle 5, Schedule 1) requires that data shall not be kept for longer than is necessary for the purpose(s) for which they are processed. In health care, expectations vary tremendously. Until recently, the advice issued to community pharmacists by the Royal Pharmaceutical Society was that PMRs up to 13 years old could be relevant to meet possible liabilities under personal injury and consumer protection law.²⁸ The most recent advice, published in issue 25 of the Medicines, Ethics and Practice guide, now fudges the issue by saying that “the required longevity of records you keep is dependent on the information kept and requirements may change with the advent of the electronic patient record”.²⁹ In practice, most pharmacies have two or three years’ worth of PMRs readily available to indicate what has recently been prescribed to individual patients. This information is important in dealing with drug interactions, changes in treatment and inadvertent errors. ETP will allow the amalgamation of data now held in PMRs with data held in the surgery, thus creating a more complete health record.

ESTABLISHING IDENTITY

At present, possession of an NHS prescription enables the bearer to get the medicines on the prescription dispensed to him. Prescriptions are sometimes forged and bona fide prescriptions stolen, but the drugs involved are limited in number and usually obvious to vigilant and “street-wise” pharmacists who keep the problem under control. ETP should make alteration or fabrication even more difficult. In the relay model, the use of a unique prescription number (UPN) will establish the right to have a particular prescription dispensed and prevent further unauthorised supply. Although in the pilots it is intended to retain paper NHS prescriptions to verify accuracy of transmission, the ultimate goal must be for them to be abandoned. Some concern may then arise over the ability of patients to remember their UPN, particularly when (anecdotally) around one in four patients use a proxy — neighbour, relative, friend, home help or local pharmacy — to collect prescriptions on their behalf. Some of the patients whose prescriptions are presented by a proxy will be among the most vulnerable members of the community. Ways must be found to ensure that ETP does not make life more difficult for them.

CONCLUSIONS AND RECOMMENDATIONS

Nothing in the machinery of the three current ETP pilots obviously offends the provisions of the Data Protection Act 1998. It is

important to recognise, however, that pharmacists may have to establish necessity before seeking access without consent to the diagnosis or related diagnostic data held in patients’ medical records. ETP does not raise novel consent or confidentiality issues, but its advent should force pharmacists and their staff to review their understanding of the duty of confidentiality owed to patients and the limited circumstances in which sensitive personal data may be processed without explicit patient consent. Although explicit consent is not a legal requirement for participation in ETP, patients should be educated about the mechanisms and rationale of ETP. It is their intimate details that

are being electronically buzzed around, and they should understand why and how this is done, and what safeguards against abuse are in place. This process of patient (and professional) education should be a joint effort by the Department of Health and by pharmacists and their organisations. Paper prescriptions may be needed for some time after ETP is widespread. The ETP pilot evaluation process should include exploration of the impact on patients. Further research should be undertaken on the general understanding of patients about the uses made of prescription data and their expectations of confidentiality from all health professionals and their staff.

REFERENCES, SOURCE MATERIALS AND NOTES

1. R v Department of Health ex p Source Informatics Ltd (2000) Lloyd’s Rep: Med 76.
2. Appelbe GE, Wingfield J. Pharmacy law and ethics (7th ed). London: Pharmaceutical Press; 2001. p371.
3. Appeal Court rules that pharmacists can sell script data. Pharm J 2000;264:5.
4. Hazlet TK, Bach MHM. The internet, confidentiality and the pharmacy.coms. Cambridge Quarterly of Healthcare Ethics 2001;10:157–60.
5. Hirst JE, John DN, Bloor MJ, Walker R. Analysis of focus group discussion on privacy in community pharmacies. Pharm J 1999;263(Suppl):R38.
6. Auguste V, Guerin C, Hazebroucq G. Opinions and practices with regard to confidentiality in French hospital pharmacies. Int J Pharm Pract 1997;5:122–7.
7. Consumers Association. Patients records should stay private says new survey 14 May 2002 and related press releases. Available at: <http://www.patients-association.com/press/press.htm> (accessed 12 June 2002).
8. Alder Hey: reports at a glance. Available at: http://news.bbc.co.uk/hi/english/health/newsid_1144000/1144373.stm (accessed 12 June 2002).
9. Alder Hey organs scandal. Available at: <http://society.guardian.co.uk/alderhey> (accessed 12 June 2002).
10. <http://www.doh.gov.uk/consent> (accessed 12 June 2002).
11. <http://web.bma.org.uk/> (accessed 12 June 2002). [Enter “consent” in “search”]
12. <http://www.doh.gov.uk/pharmacy/etp.htm> (accessed 12 June 2002).
13. <http://www.ppa.org.uk/news/etp.htm> (accessed 12 June 2002).
14. Wingfield J. The Data Protection Act 1998. Pharm J 2000;265:131.
15. Data Protection Act 1998 s. 2(e)
16. Data Protection Act 1998 s. 69(1)(d): “In this Act “health professional” [includes] a registered pharmaceutical chemist as defined by s. 24(1) of the Pharmacy Act 1954 or a registered person as defined by Article 2(2) of the Pharmacy (Northern Ireland) Order 1976.
17. Undermining privacy in health information. BMJ 2001;322:442–3.
18. Pharmacists told “reveal patient information or be fined £5,000”. Pharm J 2002;268:673.
19. Private Eye 2002;(31 May–13 June):10.
20. The Health Service (Control of Patient Information) Regulations 2002 SI No.1438
21. Principles to underpin electronic prescribing put forward by the professions. Pharm J 1997;258:755.
22. <http://www.fip.org> (accessed 12 June 2002). [Click on “statements, guidelines and position papers”]
23. <http://www.exist.nl/pdf/e-prescription-English.pdf> (accessed 12 June 2002).
24. Data Protection Act 1998 s. 1(1).
25. Data Protection Act 1998 s. 1(4).
26. Cambridge Health Informatics report. Executive summary. Available at: <http://www.doh.gov.uk/ipu/confiden/gpcd/exec/gpcdexec.pdf> (accessed 12 June 2002).
27. Building the information core. Protecting and using confidential patient information: A strategy for the NHS. December 2001. Available at: <http://www.doh.gov.uk/ipu/confiden/strategyv7.pdf> (accessed 12 June 2002).
28. Royal Pharmaceutical Society. Medicines, Ethics and Practice — a guide for pharmacists (number 24). London: The Society; 2000. p104.
29. Royal Pharmaceutical Society. Medicines, Ethics and Practice — a guide for pharmacists (number 25). London: The Society; 2001. p101.

FURTHER READING:

1. Montgomery J. Health care law. Oxford: Oxford University Press; 1996.
1. Foster C, Peacock, N. Clinical confidentiality. Sudbury, Suffolk: Monitor Press; 2000.